A SYSTEM AND METHOD FOR BIOMETRICALLY-INITIATED REFUND TRANSACTIONS

[0001] This application is a continuation-in-part of application no. 10/251,305, filed September 20, 2002, which claims domestic priority from provisional application no. 60/324,229, filed September 21, 2001. Each above-identified application is incorporated by reference herein, in its entirety, for all purposes.

FIELD OF THE INVENTION

[0002] This application relates generally to a system and method of conducting biometrically-initiated refund transactions. More particularly, the present invention relates to a system and method for allowing individuals to store and retrieve transaction information by means of biometric association.

BACKGROUND OF THE INVENTION

[0003] Generally, an individual conducting a purchase transaction receives a paper record that displays information about the transaction, such as the date of the transaction, the location of the transaction, items/services purchased in the transaction, and how the individual paid for the purchase. Should the individual wish to return a purchased item/service from that transaction for money, the individual must typically present the paper record they received of the transaction for the purposes of providing proof of the transaction, and/or necessary return details of the transaction. Requiring a customer to keep track of these paper records and present them in a refund transaction poses a nuisance to the customer that might discourage the customer from seeking a refund if they cannot find the proper paperwork.

[0004] Since retail stores are not required by law to provide customers with refund services, they may set their own refund policies. Because fraudulent refund transactions can pose a large area of risk, merchants typically enforce refund policies that help minimize these loss risks but still enable customers to return unwanted and/or defective merchandise. For example, such policies typically include requiring customers to present physical receipts for full refunds and to return purchased items within a set timeframe. Additionally, merchants often require customers conducting refund transactions to provide personal information, such as their home address, telephone number, and email address. Although paper receipts provide customers the benefit of

allowing them to conduct full refunds, keeping track of these receipts is cumbersome for customers, forcing them to keep a backlog of paperwork on their purchases and then forcing them to find a receipt in that backlog every time they want to return an item/service. In addition, requiring customers to provide personal information is not only an inconvenience to customers but also an invasion of privacy. What is needed are better systems and methods for providing customers and merchants with records of purchase transactions.

SUMMARY OF THE INVENTION

[0005] The present invention addresses the aforementioned needs by providing customers and merchants with a more accessible system and less cumbersome method of recording and accessing transaction information, wherein transaction information is stored in electronic transaction records that are accessed and updated via biometric recognition and/or verification. A process by which customer biometric information is associated with electronically captured transaction information allows customers and merchants to perform more secure, convenient, and efficient refund transactions. Additionally, a process by which customers verify their identity as purchaser or their affiliation with the purchaser of a refund transaction, offers merchants a more secure method of conducting refund transactions.

BRIEF SUMMARY OF THE DRAWINGS

[0006] **FIG. 1** illustrates an overview of the general architecture of a system for biometric authorization for refund transactions according to an embodiment of the present invention.

[0007] **FIG. 2** illustrates a flowchart of a process for creating a biometrically associated, electronic transaction record.

[0008] **FIG. 3** illustrates a flowchart of a process for conducting a refund transaction with a biometrically associated, electronic transaction record.

DETAILED DESCRIPTION OF THE INVENTION

[0009] Additional objects and advantages of the present invention will be apparent in the following detailed description read in conjunction with the accompanying drawing figures.

[0010] As previously noted, the present invention encompasses a system and method for conducting refund transactions via biometrically-initiated access of electronic transaction records.

[0011] User transaction information is stored as one or more electronic records that are associated with a user's biometric sample. Transaction information may be stored as an electronic record during or after a transaction takes place. Additionally, transaction information may be converted from physical form, e.g. a paper receipt, to electronic form at a system device, or may be pulled from one or more storage locations to a system database. Regardless of how transaction information is entered into the system, it is stored in electronic form and in association with a user biometric sample. Depending on the embodiment of the system, stored transaction information may be organized according to varying forms. By way of illustration but without limitation, transaction information may be grouped by transaction, by an item/service identification code, by an item/service related department, by price, by merchant, by merchant location, and/or by item/service description.

[0012] Storing transaction information in electronic form and in association with a user biometric sample allows a user to conduct refund transactions based upon the stored transaction information simply by presenting a biometric. Because most merchants currently require individuals to present a physical transaction receipt in a cash-back refund transaction, the present invention will provide users with a more convenient method of presenting those transaction records, by presenting their electronic transaction records in lieu of traditional physical receipts. The current invention also provides customers with greater privacy, allowing them to conduct return transactions without necessarily having to share their personal information with merchants with which they conduct return transactions. Additionally, the invention will provide merchants with a more secure form of conducting refund transactions by associating customer biometric information with a transaction. Allowing users to present electronic transaction records in a refund transaction eliminates the need for users to keep track of and present traditional physical transaction records, such as paper receipts, at the time of a refund transaction.

[0013] A user conducts transactions in the system by presenting a biometric sample that is compared to one or more registered biometric samples stored at the system database. Matching a user biometric sample to a registered biometric sample enables a user to retrieve information stored in association with the registered biometric and/or approval of a transaction request depending on the action the user requests in the system. There are two main types of biometric comparison systems: biometric verification systems, wherein the system performs a "one-to-one" comparison of an individual's biometric to a record of his biometric, and biometric recognition

systems, wherein the system performs a "one-to-more than one" biometric comparison of an individual's biometric to his biometric record and at least one other biometric record. A "one-to-one" biometric comparison verifies the individual presenting the biometric is who he says he is, and a "one-to-more than one" biometric comparison recognizes an individual's biometric from a group of two or more biometrics. For the purposes of this application, "biometric system" is intended to refer to both verification and recognition biometric systems. As would be appreciated, the invention methods and their related methods of biometric comparison disclosed herein should not be used to limit the scope of the invention. The scope of the invention should allow for varying combinations of methods and their related methods of biometric comparison.

[0014] Additionally, this invention is not limited to using one form of biometric. For example, the biometric samples referred to throughout this description might refer to an image of a biometric and/or a mathematical representation of the biometric sample, often referred to as a "template" in terms of biometric applications.

[0015] **FIG. 1** illustrates a general architecture overview of a biometrically-initiated refund system **100** that is based on biometric recognition and/or verification. As will be described in greater detail below, refund system **100** enables a receiptless refund transaction by which users are encouraged to associate their biometric information with their purchase transaction information. Transaction information is stored in at least one system database **112, 114** where system user records are stored. In one embodiment, the system database is a central database to which all system user records are stored and from which informational system user records are accessed for identity verification/recognition. In another embodiment, the system database is one or more operator databases **114** to which a select set of user records are stored and from which a select set of user records are accessed for identity verification/recognition. In an additional embodiment, refund system **100** may also utilize a combination of central databases **112** and one or more operator databases **114**. In general, embodiments utilizing a combination of system databases **112, 114** enable increased control of information flow throughout the refund system **100**. As described in greater detail below, various examples of information flow configurations within the system can include "open," "closed," and "selectively shared" system models. In still further embodiments, system database **112, 114** can further comprise one or more sub databases that are contained within a particular system database **112, 114**. In such embodiments, system user data, system operator data, and other system data may be distributed

across multiple databases within the system database.

[0016] A system user record holds system user biometric information and other identity verifying information related to an individual seeking biometric recognition/verification so that the system user may identify himself and associate his transaction information with his system record. The information held in such a record may include, by way of illustration and without limitation, a system user's government identification number(s) and corresponding state(s) of issue, home address, a telephone number, and at least one biometric record. A system user may present any number of identity verifying documents or testaments to his identity depending on the embodiment of the biometric system. By way of illustration and not of limitation, examples of such documents or testaments include a financial token, a digital image, a video clip, family information, or a DNA sample. Depending on the particular implementation, a system user record can also hold financial account information and/or a system identification number (SID). A SID is a code used in conjunction with a system user biometric sample for biometric recognition/verification.

[0017] The system also comprises system operator records which hold information useful for authenticating an operator, such as a name or ID number, device ID numbers associated with the operator, an address, and a phone number. In an alternate embodiment of the present invention, the operator records also hold employer information if the operator is an employee of an employer who is also an operator. In another embodiment of the present invention, operator records hold an operator SID and/or an operator biometric sample.

[0018] The system may be configured so that at least one system database **112, 114** is connected to at least one network **102**, such as but not limited to, the Internet. This network comprises connections to at least one device where transaction information is entered. These devices include but are not limited to a vending machine **152**, a kiosk **156**, a personal computer **132**, a user service desk **160**, a point of sale (POS) terminal **164**, or a wireless device **144, 140,** and **136**, connected via wireless network **104**, with respective biometric input devices (BIDs) **130, 134, 138, 142, 146, 154, 158, 162** and **166**. BID devices are illustrated in **FIG. 1** as peripheral devices for purposes of emphasis only. The system should not be so limited and may certainly incorporate devices with built-in BIDs.

[0019] Networks used in additional embodiments include LANs (local area networks), WANs

(wide area networks), and telephone networks. In such embodiments, system users communicate with at least one system database **112, 114** via telephone **128,** with connected BID device **130.**

[0020] Additional embodiments of the system also comprise connections to one or more third party sources, such as a third party database **106** and/or one or more financial institutions **108,** in which system user-presented information is verified and/or from which system user information is pulled. Financial institution **108** may also allow users to conduct biometrically authorized financial transactions with the system should the system be so configured. For ease of integration of such methods, the method of conducting biometrically authorized financial transactions might be adapted so that it may be conducted concurrently with the method for biometrically initiated refund transactions and vice versa.

[0021] In one embodiment, the system is configured as an "open" system, meaning all information entered into the system is transmitted to and stored in a central system database **106.** An open system allows system user transaction information to be stored and/or accessed via any device in the system because an open system shares system user information stored in the centralized system database **112** with all system devices. System user records in an open system may additionally be sub partitioned by system operator with which the user conducts transactions. This system embodiment allows user identity information to be shared across system operators freely but restricts access to operator-specific sub partitions within the user's record to the specific system operator and his associated system operators.

[0022] In an alternate embodiment, the system is configured as a "closed" system, meaning information entered into the system via a specific operator device is transmitted to and stored in a system database specific to that operator **114,** and this information is not shared with devices other than those specific to the operator database **114** or other operator-specific databases. This is referred to as a "closed" system because system user information stored in one system operator's database **114** is unique to that user's interaction with that specific system operator and/or specific system operator device(s). System users must register their identifying information in the database of each additional system operator system wherein they would like to store electronic transaction information. Operator system databases **114** in closed systems may query other databases, such as a third party information database **106,** for system user information verifications. However, all system user information that is enrolled into a particular operator system database **114** is stored in that database. In an alternate embodiment of the closed

system, information pertaining to specific system operators is stored in a partitioned, central system database **112**. System operator related information is stored in system, operator-specific partitions and is closed to all other system operators. Only the system operator and system operator employees may access that partition of the central system database **112**. In yet an additional embodiment, system operator related information stored in an operator system database is additionally stored on the central system database **112** where their system users' records are stored. Such an embodiment is useful for information protection in the event database information is lost.

[0023] In a further embodiment of the present invention, system user information is "selectively shared" and stored in select system multiple-operator databases or select, system multiple-operator partitions within the central system database **112**. In this embodiment, a group of system operators share data with each other and they choose whether or not to share system information with other system operators within the system. Such a system is referred to as a "selectively shared" system. This system allows a chain of system operators owned by the same entity or linked in some other manner to share system user information amongst them without sharing that information with all other non-designated system operators registered in the system. Information in such a system may be shared between one or more operator system databases **114** and the central system database **112** freely or sharing may be monitored by rules set in the operator system databases **114**, the central system database **112**, or both. By way of illustration and not as a limitation, one system operator might only want to share system user transaction information with one of five system operators in a multi-verifier system or all system operators might not want to send or store system user transaction information to the central system database **112**. Such a system allows system operators greater control over information flow while still allowing various user conveniences, such as being able to return a product to any store in a selectively shared chain.

[0024] The configuration of the system as an "open" system, "closed" system, or "selectively shared" system illustrates various ways of implementing the principles of the present invention. System configuration might be determined by the system in which the electronic transaction information is used. For example, if the refund system is combined with a biometrically-authorized financial transaction system, a merchant who is an operator in the system and who allows customers to conduct biometrically-authorized financial transactions might have a system

configured with his own operator system database **114** and one or two biometric authorization terminals, for example **164** and **160**, connected to that database. In this system configuration, the merchant's database files only exist on his database **114** and are retrieved or accessed for biometric matching only by the one or two pre-determined stations **164** and **160** connected to the database **114**; therefore, the system would be a "closed" system.

[0025] System users register for a biometrically-initiated refund transaction system by creating a user record with a system database. As would be appreciated, determining the data required to enable usage of the system would depend on the embodiment of the system. However, in a standard enrollment, a user presents at least one biometric sample. A user may additionally present other identity verifying information, such as his name, mailing address, phone number, driver's license number, and e-mail address. Depending on the system embodiment, the system may additionally require a user to register a system identification number (SID). In such an embodiment, a SID typically serves as a pointer that can be used with or without a user biometric sample to aid the system in locating the storage location of a user record. Depending on the embodiment of the system, a SID may also serve as a user group identifier that identifies a user as an affiliate of a specified group of users. In an additional embodiment, the system may perform a re-registration check on a user's information to ensure that the user is not already registered in the system.

[0026] Regardless of the information required for enrollment, users may enroll in the system in an enrollment transaction or may enroll in the system during another system transaction. For example, a user who wishes to enroll in the system presents his biometric information and any other requested identity information. That user's information is stored in a database, and the user is enrolled. The user may, alternatively, wish to enroll in the system during a purchase transaction. For example, a user purchasing a few items at an electronics store might decide that she would like to enroll in the system. If she chooses to enroll, she would then enter a biometric sample. She would additionally enter any other enrollment information that the system requests. The method of entering such information would be implementation dependent. For example, information could be hand-keyed, pulled from an electronic read of a token, and/or pulled from another information database, which may or may not be designated by the user. The current transaction information is then associated with the user biometric sample, both of which are stored in a system database as a user record. Thereafter, the user simply provides her biometric

sample during a transaction and the transaction information is stored with the user's system record.

[0027] In an additional embodiment, the present invention is combined with a biometrically-authorized transaction system that requires a user to present his biometric during a transaction for identity verification, such as a biometrically-authorized financial transaction system, an age-restricted transaction system, or a rewards transaction system. The present invention used in combination with such a system would enable the transaction information to be stored in association with a user identity-verification record previously created for enrollment into the additional biometric system.

[0028] In yet another embodiment, a user wishing to convert pre-existing physical and/or electronic records of transaction information into the system may present these records at a system device. The system device would scan and/or read the records, retrieving them from transaction information to be stored in association with the user's system record. If a user is not enrolled in the system, he may still convert a pre-existing record of a transaction into the system in the process. He simply presents his biometric, the transaction information, and any other necessary enrollment information, and this information is sent to a system database for storage as a new user record.

[0029] **FIG. 2** illustrates a method by which transaction information is entered into and stored in a system for creating electronic transaction records.

[0030] At step **202**, information related to a transaction is entered into a transaction station. Transaction information may include but is not limited to, the date of a transaction, the time of a transaction, the location of a transaction, one or more items/services exchanged in a transaction, the quantity of one or more items/services exchanged in a transaction, the price of one or more items/services exchanged in a transaction, the method of payment in a transaction, and one or more system operator associated with a transaction. In an additional embodiment, the method of creating an electronic transaction record is appended to a method for biometrically authorizing a transaction. In systems wherein such methods are combined, transaction information may additionally include a transaction approval request that is evaluated and approved or denied concurrently with the method of storing the electronic transaction record.

[0031] At step **204**, the transaction information and a user biometric sample is sent to a system

database. The user biometric sample may be scanned into the transaction station at any time during the transaction. Additionally, if the current invention is appended to a biometrically authorized system and method, the biometric sample captured for use in authenticating the user to that authorization system may be also used in the method of the current invention. In an additional embodiment, the system is configured for biometric verification and might request a user additionally enter a system identification code (SID) that is also sent to the database. In a biometric verification embodiment, a SID may serve various purposes. For example, it can be used as added insurance that the user is properly identified within the system database, or it can serve as an affiliation code by which a group of users affiliate their electronic transaction records with each other in an effort to create a chain of possible users authorized to conduct refund transactions for their purchase transactions. Regardless of the purpose of the SID, such an embodiment of the system would help simplify and increase reliability of the system by increasing the probability that the user's electronic transaction record is stored in the proper user record. It is also possible at this point that the user enters a transaction code that indicates user-defined categories of transactions. For example, if the user is making a business purchase, he enters a code that indicates that the transaction is business related, or if the user is making a leisure purchase, he enters a code that indicates that the transaction is leisure related. Such codes might enable users to better organize their transaction records.

[0032] At step **206**, the user record is located by matching the biometric sample to a biometric sample stored at the database. If the user entered a SID, a user record might first be located by the SID and the biometric sample verified with a registered biometric sample associated with the SID. At step **208**, if the user record is located, the transaction information is stored in association with the system record. Alternatively, if no user record is found in the system one is created and the transaction information is stored in association with the newly formed record. Additionally, users who wish to receive a paper record of the transaction might select to receive one.

[0033] Depending on the embodiment of the invention, electronic records stored in association with user records might additionally be divided into sub records associated with one or more system operators. For example, in a financial transaction merchant information included in the transaction information might designate a specific sub record with which to associate the transaction record. Such an embodiment might allow for faster transaction information location during later user record accesses. Additionally, such an embodiment would serve closed or

selectively shared system organizations by requiring merchant information to be matched before allowing access to the user sub record associated with that merchant. As users may affiliate their user records with other users, so may system operators affiliate their records in selectively shared systems. In such a system, a system operator identifier would provide that system operator access to his designated group of affiliated system operators within the system.

[0034] In an additional embodiment of the system, users may utilize a personal biometric device to aid storing transaction information in the system. Such an embodiment is conceived for transactions in which a merchant does not have a biometric device but has a device that can communicate with a user personal device, such as a personal data assistant **144** with BID **146**, a pager **140** with BID **142**, and/or cellular phone **136** with BID **138**. In such transactions, transaction information is electronically communicated to the user personal device **144**, **140**, **142**, into which the user presents his biometric sample via connected/integrated BID **146**, **142**, **136**. This information is sent to the system database, where it is stored in association with the user record. Methods of communicated transaction information from the transaction terminal to a user personal device might include but should not be limited to infrared transmission and other forms of wireless communication.

[0035] The system might also allow users to create electronic transaction records after a transaction has taken place by converting conventional transaction receipts into electronic form and/or storing that new electronic form in association with a user biometric. This method might be useful to new system users who have kept a backlog of transaction receipts that they would like entered into the system. Additionally, this method might also be a useful back-up method for the electronic system should a system operator device not be functioning properly during a transaction. A user converts traditional transaction receipts to electronic form via a system device equipped for record conversion. As would be appreciated, the method of record conversion depends on the format of the original transaction receipt. For example, a paper receipt might be digitally imaged into a system device and/or scanned for optical character recognition (OCR). Other forms of receipt conversion might be as simple as a user presenting a smart card whereon the transaction information is stored and that transaction information is electronically transferred and/or copied from the card to the system database and stored in association with the user record. A system device for performing receipt conversion might be a kiosk equipped with a digital scanner and a biometric scanner. In the case of a paper transaction

receipt conversion, the user would present the paper transaction receipt into the kiosk's digital scanner for scanning and/or information retrieval. The user would also present his biometric at the kiosk biometric scanner. The kiosk would retrieve the transaction information from the paper transaction receipt and send the transaction information and user biometric sample to the system database, where the information is stored with the user system record. If the user is not registered with the system, the database forms a new user record with which the user biometric sample and transaction information is stored. Additionally, receipt information a user presents may also include a code which identifies another location where supplemental transaction, operator, or user information is stored. With this code, the system may pull any supplemental transaction information not identified on the material a user has presented. For example, a paper transaction receipt may include a code pointing to where purchaser credit card information is stored in a merchant database.

[0036] In an additional embodiment of creating an electronic record within the system, user biometric information is matched at the transaction station. In such a method, a user enters his SID, which is used to locate the user's registered biometric sample. The user's registered biometric sample is sent to the transaction station, where it is compared to the user biometric sample entered during the transaction. If the biometric samples match, the transaction proceeds. In such an embodiment, transaction information may be sent to the database with the user SID, and the bulk of the transaction may be pre-approved/pre-declined based upon system parameters, allowing the transaction to be completed with acknowledgement of matching biometric samples. Alternatively, the system may not send transaction information to the database with the user SID, and may only proceed with processing the transaction after the user biometric sample has been matched to a user registered sample.

[0037] Referring to **FIG. 3**, a flowchart of a process for an automated refund transaction is illustrated. At step **302**, a system user biometric sample and a refund transaction request is entered. The refund transaction request may include but is not limited to one or more of requesting cash back for one or more returned items/services, requesting credit for one or more returned items/services, one or more product references indicating one or more products to be returned, and system operator information. For the purposes of this application, "cash back" refers to a refund transaction in which the user requesting the refund seeks a full reimbursement of money spent on the purchased item/service that they are requesting to return. Additionally,

"credit" refers to credit a merchant typically provides a customer in place of cash back for products/services returned that may only be used at that specific merchant's or his affiliate merchants' stores. Depending on the embodiment of the system, product references may additionally be included in refund transaction requests. Such references include but are not limited to various specific product/service codes, such as universal product codes (UPCs), radio frequency identifiers (RFIDs), and infrared identifiers or various descriptive product/service references, such as product descriptors and department codes. The format in which the product code is disclosed might determine how the code is entered into the system. For example, if the code is a universal product code (UPC), which is typically printed on literature/packaging included with the product in numerical and bar code form, the code might be scanned and electronically entered. Likewise, a UPC might be hand keyed into the system by a system operator and/or user. Other formats of product code information include radio frequency identifiers (RFIDs), infrared transmitters, and/or any other form of electronic code identifiers.

[0038] At step **304**, the user biometric sample and refund transaction request are sent to a database. In an additional embodiment, the system is configured for biometric verification and might request a user also enters a SID. In a biometric verification embodiment, the SID may serve as a pointer for locating the user record within the database, may indicate that the user is affiliated with a group of users, and/or may also indicate that the user seeking a refund transaction is not the purchaser of the item/service being returned but is affiliated with the purchaser in the system. Such an embodiment allows users to conduct return transactions for items/services purchased by affiliated users, such as gifts received from affiliated users or items purchased by affiliated business associates. In such an embodiment, all user records associated with the group SID entered are scanned for information that might pertain to return transaction request information.

[0039] At step **306**, a user record is located at the database. At step **308**, user transaction information associated with the user record is located. Depending on the product/service information provided in the refund transaction request, transaction information may be located in a number of ways. For example, if a product UPC was entered in the refund transaction request, product UPCs of the items purchased by the user are scanned until a match for the presented UPC is found. Alternatively, if more generic purchase item information is included in the refund transaction request, the system locates all items purchased relating to that information. This

information is then presented to the system operator and/or the user so that the desired return information may be selected. At step **310**, the refund transaction is initiated.

[0040] In an additional embodiment, one or more refund transaction request parameters must be met before the refund is initiated. For example, the system might comprise a system operator supervising the transaction to evaluate the condition of a returned item to ensure that the item was not used/abused and then presented for return. The system might also request that the system operator record the condition of the item via hand-keyed description, digital imaging, or a similar method of capturing item condition. In yet an additional embodiment, the user record pertaining to the returned item is marked returned to indicate that the user has already received a refund for that item.

[0041] In an additional biometric verification embodiment, refund request information, a user biometric sample, and a user SID are entered into the transaction station. The user SID is sent to a system database, and the user record and associated registered biometric sample are located. The registered biometric sample is sent to the transaction station, where it is compared to the user biometric sample. In embodiments in which group SIDs are implemented, all registered biometric samples associated with the group SID are returned to the transaction station. If the user biometric sample matches a registered biometric sample returned to the transaction station, refund request information is sent to the database, where it is either evaluated and approved or where it is used to retrieve transaction information relating to the refund request that is sent back to the transaction station so the appropriate transaction information may be designated and/or verified. In yet an additional embodiment, refund request information might be sent to the database upon initial transmission, along with the user/group SID. In such an embodiment, the refund request might be pre-approved, pending biometric matching, or transaction information stored in association with the user record and relative to the refund request might be returned to the transaction station so the appropriate transaction information may be designated and/or verified.

[0042] In an alternate embodiment, the system biometric matching parameters may be relaxed in an effort to reduce the value threshold, meaning less biometric information is used for matching therefore more biometric matches may occur. Typically, reducing the value threshold in turn increases the number of false positives a biometric matching session will return. By

default, if a system can increase its number of false positives it in turn decreases its number of false negatives. The value threshold is reduced in an effort to create a larger amount of potential matches. Such a system would help ensure a more reliable consistency in pulling the matching user record on the first database scan. In a similar embodiment where a user enters a SID, the user SID may be truncated in an effort to return multiple potential biometric and transaction matching possibilities.

[0043] In an additional embodiment, users who receive a gift they would like to return may do so via the system by identifying the gift purchaser by providing purchaser information, such as a phone number. This information can then be used to retrieve the transaction record for the item the presenting user wishes to return. Record of such a return transaction would then be stored in the purchaser's and the presenting user's system record.

[0044] System operators who conduct biometrically initiated refund transactions might also want a method for encouraging customers who are not system users but who are seeking a refund to enroll in the system. In order to do so, system operators might implement a method of conducting receiptless refunds in conjunction with enrollment methods. A receiptless refund is a refund transaction request in which a customer seeks a refund for a transaction for which they have no transaction record to present. Such a user may not be enrolled in the system or may not have used the system during the specific transaction involved in the refund request. Should the customer not be enrolled in the system, the merchant might require the customer to enroll in the system by presenting at least a biometric sample. Depending on the embodiment of the system, the customer might present additional information such as but not limited to his name, address, telephone number, driver's license number and state of issue, financial account information, a SID, and any other identity information typically entered in a receiptless refund transaction. These types of transactions might provide system operators with some security in providing receiptless refunds because they provide merchants with at least biometric information. System operators desiring additional security might also associate system parameters with such transactions. For example, a system operator might only allow a customer to perform two receiptless refunds at that merchant's store over a specified period of time. Additionally, a system operator might not wish to provide a customer seeking a receiptless refund with a complete refund for the item they are returning and might set a system parameter in which the customer only receives a percentage of the requested refund for the returned item. Additionally,

some system operators might wish to only extend store credit to users requesting receiptless refunds. In such a transaction, the system might additionally be configured to refund a user's money by associating a stored value account with the user that the user may use via biometric authentication.

[0045] Users may additionally access their system records for maintenance and user services such as refund request pre-approvals. Users may access their records by presenting a biometric sample and/or a SID. Access may be provided at a number of devices, including user personal devices, such as a personal computer **132**, a telephone **128**, and a user wireless device **136, 140, 144**. Users may access their system records to track their transactions, update their user information, customize their user record, and/or request a refund transaction pre-approval. An example of how a user might track his transactions would be his provision of transaction codes to label and organize his electronic transaction records within the system according to the purpose of the transaction. For example, if the user is making a business related purchase, he might mark the transaction with a business code, or if the user is making a leisure related purchase, he might mark the transaction with a leisure code. Such a system may allow users to sub-divide their transactions according to these user-set transaction codes. Additionally, a user may request a refund transaction pre-approval by accessing his transaction records, locating the record(s) pertaining to his desired return transaction, and marking the record(s) with a request for refund. Once the system has pre-approved the refund transaction, the user need only return to the store or a refund kiosk, where he deposits the item(s) and where his refund request is approved. Such a method allows users and system operators to save time in completing return transactions.

[0046] In an additional embodiment, information transferred between two points in the system is encrypted. For purposes of example and without limitation, information may be encrypted at one point and sent across a non-secure connection between the points or not encrypted at a point of communication and sent to the other point of communication across a secure connection. Various methods of encryption and decryption may be used, and the embodiment should not be limited to one type of encryption. For example, the system may incorporate one or more methods such as SSL encryption, methods used by companies such as Verisign, PIN encryption typically used in a Point of Sale debit transaction, and/or any other similar method of encryption. As an added level of security, one alternate embodiment encrypts information internal to a terminal and which is never transmitted in a communication. This prevents retrieval of sensitive

information (*e.g.*, data corresponding to a biometric scan) from a stolen terminal. In an additional embodiment, the system incorporates one or more anti-tampering methods by which to recognize authentic and non-authentic system requests.

[0047] It is also an alternate embodiment of the present invention to provide operators with system user and other operator profile reports in case of suspected fraudulent activity within the system. These reports may be customized to display selected information from a system user's or system operator's record.

[0048] In an additional embodiment, user system access may be revoked. If for example the user has displayed negative system behavior, a user's usage might be revoked by deleting the user's system record from the database, marking a user's system record as in bad standing with one or more system operators, or marking the user's record as in bad standing with the network and/or one or more system operators and designating a period of time for which the record will remain bad. This period of time might be relative to an action that must be performed by the user with the record marked in bad standing.

[0049] A system and method for conducting electronic refund transactions in a biometric identification/verification system has been illustrated. It will be appreciated by those skilled in the art that the system and method of the present invention can be used to perform more convenient and more secure refund transactions than those offered by traditional methods of refund transactions. It will thus be appreciated by those skilled in the art that other variations of the present invention will be possible without departing from the scope of the invention disclosed.

[0050] These and other aspects of the present invention will become apparent to those skilled in the art by a review of the preceding detailed description. Although a number of salient features of the present invention have been described above the invention is capable of other embodiments and of being practiced and carried out in various ways that would be apparent to one of ordinary skill in the art after reading the disclosed invention, and therefore the above description should not be considered to be exclusive of these other embodiments. Also, it is to be understood that the phraseology and terminology employed herein are for the purposes of description and should not be regarded as limiting.